До разової спеціалізованої вченої ради
Національного університету
«Одеська юридична академія»

РЕЦЕНЗІЯ

рецензента, доцента кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидата технічних наук, доцента ***Ахметьєвої Ганни Валеріївни***

на дисертацію ***Дикої Анастасії Іванівни*** на тему: **«Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення»**, подану на здобуття ступеня доктора філософії за спеціальністю 122 “Комп’ютерні науки”

Актуальність теми дисертаційного дослідження. Світові тенденції розвитку цифрових технологій та міжнародні й державні стратегії, спрямовані на цифрову трансформацію в усіх сферах людської діяльності та забезпечення фінансової прозорості, сприяють масштабному розвитку IT-індустрії, зокрема розробленню вебзастосунків. На відміну від вже застарілих вебсторінок з статичним наповненням, сучасний вебзастосунок – це комплексний складний програмний продукт, який пов’язує бази даних, системи зберігання даних, засоби аналізу і моніторингу подій, різні системи взаємодії з клієнтами, засоби управління, оновлення та візуалізації контенту. І це ще не повний спектр функціональності вебресурсів.

Разом з підвищенням складності програмної складової вебресурсів зростає ймовірність помилок при проєктуванні та розробці системи, можливі випадки неузгодженості компонентів при вдосконаленні та оновленні даних, при міграції баз даних, деякі системи зберігання та обробки даних не працюють з максимальною ефективністю. Разом з проблемами, що виникають при розробці вебзастосунків, розвиваються новітні атаки, найвідоміші з яких: DDoS-атаки, SQL-ін'єкції, порушення контролю доступу, міжсайтовий скриптинг, підробка міжсайтових запитів, а також до них додаються численні фішингові схеми, що залучають значні фінансові ресурси, адже вигода зі скоєної зловмисної дії набагато вища.

Зростання мультимедійного контенту у вебресурсах сприяє поширеному використанню стеганографії, спрямованої на подолання засобів моніторингу

мережевого трафіку та організацію каналів прихованої комунікації, що вимагає додаткового тестування цифрових даних на наявність прихованих вкладень. І якщо раніше особливої потреби в такій перевірці не було через недостатнє поширення або нестійкість стеганографічних методів до атак, то в сучасних умовах зросла якість методів вбудовування, які забезпечують високу стійкість до стиснення, фільтрації, накладанню шуму та інших спотворень, а також збільшується обсяг платформ обміну мультимедійними даними, що надає величезні можливості розгортання прихованих каналів зв'язку.

Таким чином, виявлення недостовірних вебзастосунків та стеганографічних каналів у вебресурсах має важливу практичну цінність, оскільки сприятиме очищенню Internet-простору від небажаних інцидентів, спрямованих на порушення цілісності, конфіденційності та доступності інформації. Інтеграція методів стеганоаналізу та виявлення фішингових сайтів в сучасні системи тестування безпеки вебзастосунків як на етапі розробки, так і протягом усього життєвого циклу ресурсів дозволить знизити ступінь зловживань та шахрайських наслідків, а це в свою чергу підвищить довіру клієнтів і користувачів до цифрової трансформації.

Ступінь обґрунтованості наукових рекомендацій, положень і висновків, сформульованих у дисертації. Дисертаційне дослідження характеризується системним та послідовним підходом до вивчення предмету – теоретичних основ та методів виявлення прихованих каналів і фішингових атак у вебзастосунках.

Метою роботи є підвищення ефективності виявлення фішингових атак та прихованих стеганографічних каналів у вебзастосунках шляхом розробки теоретичного базису та методів тестування безпеки на основі перетворення Уолша-Адамара і методів машинного навчання, придатних для інтеграції у CI/CD-середовище.

Для досягнення зазначеної мети у дисертації вирішувались такі завдання: проаналізувати сучасний стан проблеми щодо вразливостей вебзастосунків, зокрема загроз фішингових атак та створення прихованих каналів передачі інформації засобами стеганографії в контексті життєвого циклу розробки програмного забезпечення (CI/CD) та процесів тестування безпеки; розробити теоретичний базис для виявлення прихованих каналів, побудованих на основі концепції кодового управління, шляхом аналізу статистичних властивостей трансформант перетворення Уолша-Адамара; узагальнити розроблений теоретичний базис виявлення прихованих каналів у просторі перетворення Уолша-Адамара на випадок каналів, створених за допомогою SVD UV-методів, через аналіз характерних зсувів у їхньому спектрі; розробити методи стеганоаналізу на основі машинного навчання для виявлення стеганографічних

повідомлень, сформованих сучасними методами (зокрема з кодовим управлінням та SVD UV), орієнтованих на роботу у реальному часі та інтеграцію у Runtime Security вебзастосунків для тестування мультимедійної інформації, що надходить від користувачів; формувати ансамблеві підходи до стеганоаналізу сучасних стеганоалгоритмів шляхом інтеграції розроблених теоретичних засад та сучасних алгоритмів машинного навчання з подальшим дослідженням їхньої точності, стійкості та швидкодії при виявленні прихованих каналів у вебзастосунках; виконати інтеграцію алгоритмів штучного інтелекту та машинного навчання у процедури автоматизованого тестування безпеки вебзастосунків з метою створення адаптивних методів виявлення фішингу з високою точністю детектування; провести порівняльний аналіз ефективності запропонованих методів із відомими аналогами за базовими критеріями у контексті тестування безпеки вебзастосунків; розробити підходи до інтеграції запропонованих стеганоаналітичних методів і методу захисту від фішингу у життєвий цикл вебзастосунків у межах концепції DevSecOps.

Методологічним підґрунтям дисертаційного дослідження виступає комплекс загальнонаукових та спеціальних методів наукового дослідження. За допомогою загального підходу до аналізу стану й технології функціонування інформаційних систем (ЗПАІС), методів матричного аналізу, спектрального та сингулярного розкладу, теорії інформації та кодування, теорії досконалих алгебраїчних конструкцій було розроблено теоретичний базис захисту вебзастосунків від прихованої комунікації (розділ 2). Методи теорії сигналів, статистичного аналізу та машинного навчання дозволили розробити стеганоаналітичні методи виявлення стеганографії на основі модифікації трансформант дискретного косинусного перетворення, сингулярного розкладу та перетворення Уолша-Адамара (розділ 3). Моделі виявлення фішингових атак і адаптивні методи безпеки вебзастосунків були побудовані з використанням методів машинного навчання та штучного інтелекту (розділ 4). Для оцінки ефективності запропонованих методів були застосовані методи математичного моделювання, теорія алгоритмів і методи статистичної оцінки стохастичної якості (п.3.4, 3.5, 3.7, 4.5).

Обґрунтованість роботи підтверджується опрацюванням дисертанткою значної кількості наукових праць, а також широкою базою нормативних та емпіричних джерел. Наведене також свідчить про всебічне вивчення проблематики роботи, високий рівень наукової підготовки дисертантки та її спроможності до систематизації сучасних підходів в задачах безпеки вебзастосунків, що дозволяє підвищити рівень аналізу вебресурсів на наявність актуальних проблем. Результати дослідження свідчать про виконання

поставлених наукових задач, є логічними та послідовними, аргументованими та новими для інформаційних технологій.

Рівень виконання поставленого наукового завдання та оволодіння здобувачем методологією наукової діяльності. Дисертація складається із анотації, переліку використаних скорочень, вступу, чотирьох розділів, які включають двадцять чотири підрозділи, висновків, списку використаних джерел (237 найменувань) та двох додатків. Структура дисертації Дикої А.І. не викликає заперечень. Виклад змісту дисертації логічний та послідовний.

У вступі обґрунтовано актуальність теми наукового дослідження, означено зв'язок дисертаційної роботи з науковими програмами і державними стратегіями, сформульовано мету роботи та завдання дослідження, подано коротку характеристику результатів дослідження, їх наукову новизну та практичне значення, ступінь їх апробації та публікації.

У першому розділі досліджено взаємозв'язок поняття цифрової трансформації з розробкою вебзастосунків, роль тестування безпеки вебзастосунків та основні інструменти тестування безпеки у вебпросторі, визначено основні загрози вебзастосункам, а також обґрунтовано необхідність захисту вебресурсів від фішингових атак та каналів прихованої передачі даних.

У другому розділі детально досліджено основні поняття і математичний апарат стеганографії з кодовим управлінням та на основі SVD UV-методу, проаналізовано, як впливає кодове управління на властивості трансформант перетворення Уолша-Адамара, підготовлено теоретичний базис для виявлення стеганоповідомлень, сформованих SVD UV-методом.

В третьому розділі розроблено три стеганоаналітичних методи для виявлення вкладень в цифрові зображення на основі методу кодового управління та SVD UV-методу, а також проведено порівняння результатів експериментів з аналогами.

У четвертому розділі проаналізовано сучасні фішингові атаки на вебресурси та підходи, спрямовані на виявлення підроблених сайтів, а також запропонований метод детектування фішингових вебсторінок на основі SVM та візуалізації HTML, проводиться порівняння запропонованого підходу з сучасними аналогами. В останньому підрозділі пропонується архітектурна модель інтеграції модулів стеганоаналізу та виявлення фішингу в контур Runtime Security.

Всі поставлені завдання у дисертаційній роботі виконано в повному обсязі, зроблено відповідні висновки щодо ефективності запропонованих методів, які рекомендовано інтегрувати в сучасні інтелектуальні засоби тестування безпеки на всіх етапах життєвого циклу вебзастосунків.

Повнота викладених наукових положень в опублікованих працях. Основні наукові положення дисертації, висновки та рекомендації Дика А.І. достатньо повно представила в двадцяти восьми наукових публікаціях, у тому числі в одинадцяти статтях, опублікованих у наукових фахових виданнях, перелік яких затверджено МОН України, одній колективній монографії, двох навчально-методичних посібниках, опублікованих у співавторстві з науковим керівником, тринадцяти тезах доповідей на науково-практичних конференціях, а також отримано авторське свідоцтво на комп'ютерну програму «Black Sea Hanter» (№ 129198 від 21.08.2024).

Теоретична та практична значимість результатів дисертаційного дослідження. Розроблені авторкою і викладені у дисертації наукові результати були реалізовані у вигляді конкретних методів та алгоритмів, які можуть бути застосовані в системах захисту інформації. Особливою характеристикою запропонованих методів є їхня обчислювальна ефективність та відносна простота алгоритмічної реалізації, що дозволяє інтегрувати їх у серверні або клієнтські частини вебзастосунків. Зокрема, були розроблені методи виявлення стеганографічних повідомлень з кодовим управлінням на основі запропонованого математичного апарату аналізу характеристик модальностей розподілу трансформант перетворення Уолша-Адамара, реалізовані у вигляді мережі Multilayer Perceptron та ансамблю згорткових нейронних мереж, що дозволило підвищити ефективність виявлення вкладень на 5,6 та 6,6% відповідно; метод виявлення прихованих каналів передавання інформації у вебзастосунках, сформованих SVD UV-стеганографією (точність виявлення стеганоповідомлень перевищує 90%); метод виявлення фішингового контенту, що базується на поєднанні побайтової візуалізації HTML-коду та машинного навчання (точність класифікації фішингових та оригінальних вебсторінок становить 92,45%). Ефективність всіх запропонованих методів доведена проведеними обчислювальними експериментами. Результати наукових досліджень було впроваджено у діяльність в IT-компанії EPAM (Акт впровадження Товариства з обмеженою відповідальністю «ЕПАМ СИСТЕМЗ» від 16 жовтня 2025 року) та у навчальний процес на факультеті кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія» (Акт впровадження Національного університету «Одеська юридична академія» від 1 вересня 2025 року).

Наукова новизна одержаних результатів Вивчення змісту дисертації Дикої А.І. дає можливість стверджувати, що всі сформульовані авторкою елементи наукової новизни, отримані в ході дослідження є доведеними та такими, що несуть в собі низку концептуальних висновків і рекомендацій, що

мають теоретичне та практичне значення. Зокрема, серед наукових результатів, які найбільше привернули увагу, слід виокремити наступні:

1. Було встановлено та доведено твердження щодо модальностей і зсувів статистичних характеристик коефіцієнтів перетворення Уолша-Адамара у цифрових зображеннях, що дозволило побудувати математичний апарат для розроблюваного методу виявлення прихованих каналів у вебзастосунках, сформованих SVD UV-стеганографією та стеганографією на основі кодового управління.

2. На основі проведених обчислювальних експериментів та доведених тверджень щодо статистичних характеристик трансформант перетворення Уолша-Адамара побудовано теоретичний базис для виявлення стеганоповідомлень, сформованих на основі концепції кодового управління та SVD UV-методів, що полягло в основу стеганоаналітичних методів для виявлення прихованих стеганоповідомлень у вебзастосунках.

3. Запропоновано нові методи виявлення прихованих каналів зв'язку у вебзастосунках через аналіз стеганоповідомлень, сформованих на основі кодового управління та SVD UV-методів, які забезпечують високу ефективність та швидкодію порівняно з аналогами.

4. Розроблено нову технологію автоматизованого виявлення фішингових сторінок у вебзастосунках, яка за рахунок поєднання методів обробки контенту та машинного навчання дозволяє враховувати структурні й семантичні ознаки у реальному часі, що не забезпечується наявними аналогами.

5. Запропоновані стеганоаналітичні методи та технологія виявлення фішингових сторінок у вебзастосунках інтегровано у життєвий цикл розробки програмного забезпечення, що дозволило розширити традиційні засоби SAST/DAST/IAST новітніми методами тестування, а також, на відміну від наявних аналогів, забезпечує комплексну інтеграцію у процеси CI/CD та DevSecOps.

Дотримання принципів академічної доброчесності. У дисертаційному дослідженні та наукових публікаціях здобувачки НЕ виявлено текстових запозичень без посилання на першоджерело, фабрикації, фальсифікації та інших порушень принципів академічної доброчесності.

Щодо конфлікту інтересів. Рецензент не має реального чи потенційного конфлікту інтересів щодо здобувачки, Дикої Анастасії Іванівни, її наукового керівника, Трофименко Олени Григорівни, та не є їх близькою особою.

Позитивно оцінюючи проведене дисертаційне дослідження, у порядку наукової дискусії необхідно звернути увагу на деяких питаннях, які потребують уточнення при публічному захисті дисертації, серед яких:

1. В тексті дисертаційного дослідження слід звернути увагу на невідповідність значень, наведених на рисунку 3.5 (п.3.4) та формули (3.2), зокрема значення TP відповідно до рисунку становить 102, а в формулі в обчисленнях використовується 192. Це впливає на результати ефективності виявлення стеганоповідомлень, значення яких мають становити *Precision* = 0.91, *Recall* = 0.96, *F1-score* = 0.93. Так само незрозуміло, як корелюють між собою рисунок 3.6 та формула (3.3) (п.3.5), а також рисунок 3.7 та формула (3.12) (п.3.7). Однак, незважаючи на зазначену невідповідність, підсумкова точність виявлення для стеганоаналітичних методів на основі обчислення огинаючої, на основі ансамблю згорткових нейронних мереж та на основі SVD UV-методу, обчислена вірно і становить 93.3%, 94.3% та 90.5% відповідно.

2. Згідно з теоретичним базисом, викладеним в п.2.6, метод виявлення стеганоповідомлень на основі SVD UV-методу, розроблений в п.3.7, позиціонується як сліпий, тобто спроможний виявляти вкладення без знання стеганографічного алгоритму, за допомогою якого було вбудоване приховане повідомлення. В роботі були проведені експерименти на визначення стеганоповідомлень, отриманих SVD UV-стеганографією, однак відсутні результати детектування стего-зображень, сформованих іншими стеганографічними методами. Порівняння запропонованого методу доцільно було б розширити, включивши до нього інші сучасні підходи до стеганоаналізу, зокрема методи, що базуються на аналізі сингулярного розкладу (SVD).

3. Згідно з порівнянням запропонованого методу виявлення фішингового контенту з наявними аналогами, наведеного в таблиці 4.1, розроблений підхід, хоч і поступається точністю виявлення, але має низку переваг, які позначено в примітках. На мою думку, враховуючи специфічні особливості розглянутих аналогів, слід було провести порівняння по окремим параметрам, зокрема точності, контенту, що аналізується, обчислювальним потужностям, що зробило б його більш повним та наочним.

Висловлені зауваження характеризують складність обраної теми й мають дискусійний та рекомендаційний характер, а тому істотно не впливають на загалом позитивну оцінку дисертаційного дослідження Дикої Анастасії Іванівни.

Резюмуючи, можна стверджувати, що дисертація Дикої Анастасії Іванівни є самостійним, завершеним науковим дослідженням, в якому авторка нестандартно підійшла до проблеми тестування безпеки вебзастосунків, розглядаючи стеганоаналіз цифрового контенту як складову серед інструментів тестування програмного забезпечення, комплексно обґрунтувала теоретичну та практичну специфіку обраної теми, а також інтегрувала розроблені методів у процеси тестування та забезпечення безпеки вебзастосунків в межах концепцій CI/CD та DevSecOps.

ЗАГАЛЬНИЙ ВИСНОВОК

Узагальнюючи викладене, дисертація Дикої Анастасії Іванівни «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення» є самостійною кваліфікаційною науковою працею, яка виконана здобувачкою особисто, містить нові обґрунтовані теоретичні та практичні результати проведених нею досліджень, що мають важливе значення для розвитку науки. Рецензована робота відповідає спеціальності 122 “Комп’ютерні науки” та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами, внесеними постановою Кабінету Міністрів України від 08 квітня 2025 року № 426), Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами, внесеними постановою Кабінету Міністрів України від 03 травня 2024 року № 507), а також Вимогам до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12 січня 2017 року № 40 (зі змінами, внесеними постановою Кабінету Міністрів України від 31 травня 2019 року № 759), а її авторка – Дика Анастасія Іванівна заслуговує на присудження ступеня доктора філософії з галузі знань 12 “Інформаційні технології” за спеціальністю 122 “Комп’ютерні науки”.

Рецензент:
доцент кафедри кібербезпеки
Національного університету
«Одеська юридична академія»,
кандидат технічних наук, доцент **Ганна АХМАМЕТЬЄВА**